Acceptable Use Statement

For The

State Area Network (GSN) and

Dept. of Military and Veterans Affairs Computing Resources

The following document outlines guidelines for use of the computing systems and facilities located at or operated by the Dept. of Military and Veterans Affairs (DMAVA). The definition of DMAVA computing facilities will include any computer, server or network provided or supported by the state Network Control Center (NCC). Use of the computer facilities includes the use of data/programs stored on DMAVA computing systems, data/programs stored on magnetic tape, floppy disk, CD ROM or other storage media that is owned and maintained by the NCC. The purpose of these guidelines is to ensure that all DMAVA users (support personnel and management) use the DMAVA computing facilities in an effective, efficient, ethical and lawful manner.

DMAVA accounts are to be used only for the purpose for which they are authorized and are not to be used for non-work related activities. Therefore, unauthorized use of DMAVA computing systems and facilities may constitute grounds for possible adverse action.

1. The DMAVA/GSN computing systems are unclassified systems. Therefore, classified information may not be processed, entered or stored on a DMAVA computing system. Information is considered "classified" if it is Top Secret, Secret and/or Confidential information, which requires safeguarding in the interest of National Security.

2. All users are responsible for protecting any information used and/or stored on/in their accounts. Consult the User Security Guide for guidelines on protecting your account and information using the standard system protection mechanisms http://www.nj.gov/military/cio/docs/Security_Policy&Procedures.pdf

3. Users are requested to report any weaknesses in DMAVA computer security, any incidents of possible misuse or violation of computer systems to the Help Desk or by sending electronic mail to the state Information Security Officer.

4. Users shall not attempt to access any data or programs contained on DMAVA/GSN systems for which they do not have authorization or explicit consent of the owner of the data/program.

5. Remote users (personnel utilizing laptops) will not access the internet using personal **Internet Service Providers**. When internet access is required it will done by dialing into the State network. This is the only authorized manner of internet access.

6. Users shall not divulge Dialup or Dialback modem phone numbers to anyone.

7. Users shall not share their DMAVA account(s) with anyone.

8. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

9. Users shall not make copies of system configuration files (e.g. /etc/passwd) for their own, unauthorized personal use or to provide to other people/users for unauthorized uses.

10. Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of systems; deprive an authorized user access; obtain extra resources, beyond those allocated; circumvent computer security measures or gain access to a DMAVA system for which proper authorization has not been given.

11. Electronic communication equipment is for authorized government use only. The access of pornographic,

gambling or other inappropriate web sites is not authorized. Government email will not be used for commercial business and/or the forwarding of chain letters. Fraudulent, harassing or obscene messages and/or materials shall not be sent from, to or stored on DMAVA systems.

12. Users shall not download, install or run security programs or utilities, which reveal weaknesses in the security of a system. For example, users shall not run password-cracking programs on DMAVA computing systems.

13. DMAVA computing systems will not be used at any time to further personal gain.

14. All workstations must remain **POWERED ON** at the end of each business day (exceptions will be made on a case by case basis). Individuals will only logoff as the user at the end of each day.

Use of the DMAVA computing systems are with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized.

Any noncompliance with these requirements will constitute a security violation and will be reported to the management of the DMAVA network and the state Information Security Officer and can result in short-term or permanent loss of access to DMAVA computing systems. Serious violations may result in civil or criminal prosecution and other adverse actions.

I have read and understand this Acceptable Use Statement for use of the DMAVA computing systems and facility and agree to abide by it.

Signature_____ Date_____

_____ _____

Printed: First Name, M. Last Name Grade/Rank

_____ _____

Organization Duty Phone